Quantum coin tossing

Won Young Hwang * and In Gyu Koh
Department of Physics, Korea Advanced Institute of Science and Technology, Yusung, Taejon, Korea

Yeong Deok Han †
Department of Physics, Woosuk University, Hujeong, Samrye, Wanju, Cheonbuk, Korea

We show that a secure quantum protocol for coin tossing exist. The existence of quantum coin tossing support the conjecture of D.Mayers [Phys.Rev.Lett.**78**, 3414(1997)] that only asymmetrical tasks as quantum bit commitment are impossible.

03.65.Bz, 42.79.Sz, 89.70+c

One of the most simple and interesting application of quantum mechanics is the quantum cryptography (QC) [1]- [14]. Among QC, the most well known and experimentally realized one is the quantum key distribution (QKD) [1]- [8]. Besides QKD, there are quantum bit commitment (QBC) [9,10], quantum oblivious transfer [11], and quantum secure computation (QSC) [12,13]. Recently, however, it has been shown that QBC is insecure [9,10]. As noted in Ref. [9], the insecurity of QBC implies the insecurity of other quantum cryptographical applications which are powerful enough to obtain the bit commitment. It was also noted in Ref. [9] that there might exist secure protocols for coin tossing and multiparty computations, because it is not known how to build bit commitment on top of them. In this Report, we show that a secure quantum protocol for coin tossing exist indeed.

First, we present a quantum protocol for coin tossing.

1) One party, Alice, prepares N (N is an integer much greater than 1) pairs of the maximally entangled states. Next, Alice sends to another party, Bob, one side particles of the N pairs while storing the other particles of the N pairs.

2) For each N particles Bob receives, he randomly performs spin-measurement along z or x axis. Next, he tells Alice only the measurement axes while keeping the outcome of the measurement.

3) Alice performs spin-measurement on each N particles she is storing, according to the axes Bob has told.

4) If Alice honestly sent the maximally entangled state to Bob, she can know all of Bob's outcomes from the perfect correlations of the maximally entangled states. Then, she announces all of Bob's outcome to him. Bob compares them with his data. If all of them coincide with his ones, Bob make sure that Alice has not cheated.

5) The final bit value (the outcome of coin tossing) is determined as the parity bit of all of Bob's outcomes.

If Alice honestly sent to Bob the maximally entangled states, there will be no problem: each outcome of N spin-measurement is random and consequently the parity bit of Bob's outcomes is also random. If Alice try to cheat by sending non-maximally entangled states, she cannot correctly predict all of Bob's outcomes. Thus, she cannot pass the test of step4. On the other hand, Bob has no way of cheating if Alice honestly follows the protocol because he only receives the quantum states. Therefore, both parties can be sure that they have not been cheated. To be more precise, let us show that the proposed protocol satisfy the four requirements for ideal quantum coin tossing presented in Ref. [14].

a) At the end of the coin tossing scheme, there are three possible outcomes: '0', '1' or 'invalid'.

b) Both users know which outcome occurs.

c) If the outcome '0' or '1' occur, Alice and Bob can be sure that they occur with prescribed probabilities, say $\frac{1}{2}$ each.

d) If both users are honest, the outcome 'invalid' will never occur.

As we have shown, if Alice try to cheat by sending non-maximally entangled states to Bob, she cannot pass the test of step4. In this case, the outcome 'invalid' occurs (including the following 'honest' case, (a) is satisfied). If Alice honestly sent maximally entangled states to Bob, then Alice can know all of Bob's outcomes with certainty. Hence, both users know the final outcome defined as the parity bit of all of Bob's outcomes ((b) is satisfied). Since spin-measurement on a particle of the maximally entangled state give random outcome with probabilities $\frac{1}{2}$, the final outcome occurs with probabilities $\frac{1}{2}$, too ((c) is satisfied). If Alice is honest, the outcome 'invalid' will not occur in this protocol given that there is no noise ((d) is satisfied) .

In the Ref. [14], it was shown that quantum coin tossing is impossible without entangled states shared by Alice and Bob. From this fact it was concluded that quantum coin tossing is impossible. For authors, it is not clear why entangled states are not to be used in quantum coin tossing. In our scheme the maximally *entangled states* are used indeed.

Quantum coin tossing, by itself, may not be an important application of QC. Even QBC is thought as a means to an end- two party secure computation. On the other

*e-mail: hwang@chep6.kaist.ac.kr
†e-mail: ydhan@core.woosuk.ac.kr

hand, in Ref. [9], it was conjectured that the impossibility of QBC is due to the asymmetry it creates and that only asymmetrical tasks are impossible. In this Report, we have shown that a quantum coin tossing protocol (which is a symmetric work) exists, supporting the conjecture . Thus, it could be that although asymmetrical (one-sided) two-party computation is impossible [13], symmetrical (two-sided) two-party computation is still possible. This problem should be further investigated.

---

[1] S.Wiesner, Sigact News **15** (1) (1983), 78

[2] C.H.Bennett and G.Brassard, in : Proc. IEEE Int. Conf. on Computers, systems, and signal processing, Bangalore (IEEE, New York, 1984) p.175

[3] A.K.Ekert, Phys.Rev.Lett.**67** (1991), 661; C.H.Bennett, G.Brassard, and N.D.Mermin, Phys. Rev.Lett.**68** (1992), 557

[4] C.H.Bennett, Phys.Rev.Lett.**68** (1992), 3121; A.K.Ekert, Nature**358** (1992), 14

[5] D.Deutsch, A.Ekert, R.Jozsa, C.Macchiavello, S.Popescu, and A.Sanpera, Phys.Rev.Lett.**77** (1996), 2818

[6] C.A.Fuchs, N.Gisin, R.B.Griffiths, C.S.Niu, and A.Peres, Los Alamos Report No. quant-ph/9701039, to be published in Phys. Rev.A

[7] E.Biham and T.Mor, Phys.Rev.Lett.**78**, 2256 (1997)

[8] A.Muller, H.Zbinden, and N.Gisin, Europhys. Lett.**33**, 335 (1996)

[9] D.Mayers, Phys.Rev.Lett.**78**, 3414 (1997)

[10] H.K.Lo and H.F.Chau, Phys.Rev.Lett.**78**, 3410 (1997)

[11] M.Ardehali, Los Alamos Report No. quant-ph/9512026

[12] G.Brassard and C.Crepeau, SIGACT News**27**, 13 (1996)

[13] H.K.Lo, Los Alamos Report No. quant-ph/9611031, to be published in Phys.Rev.A

[14] H.K.Lo and H.F.Chau, Los Alamos Report No. quant-ph/9605026